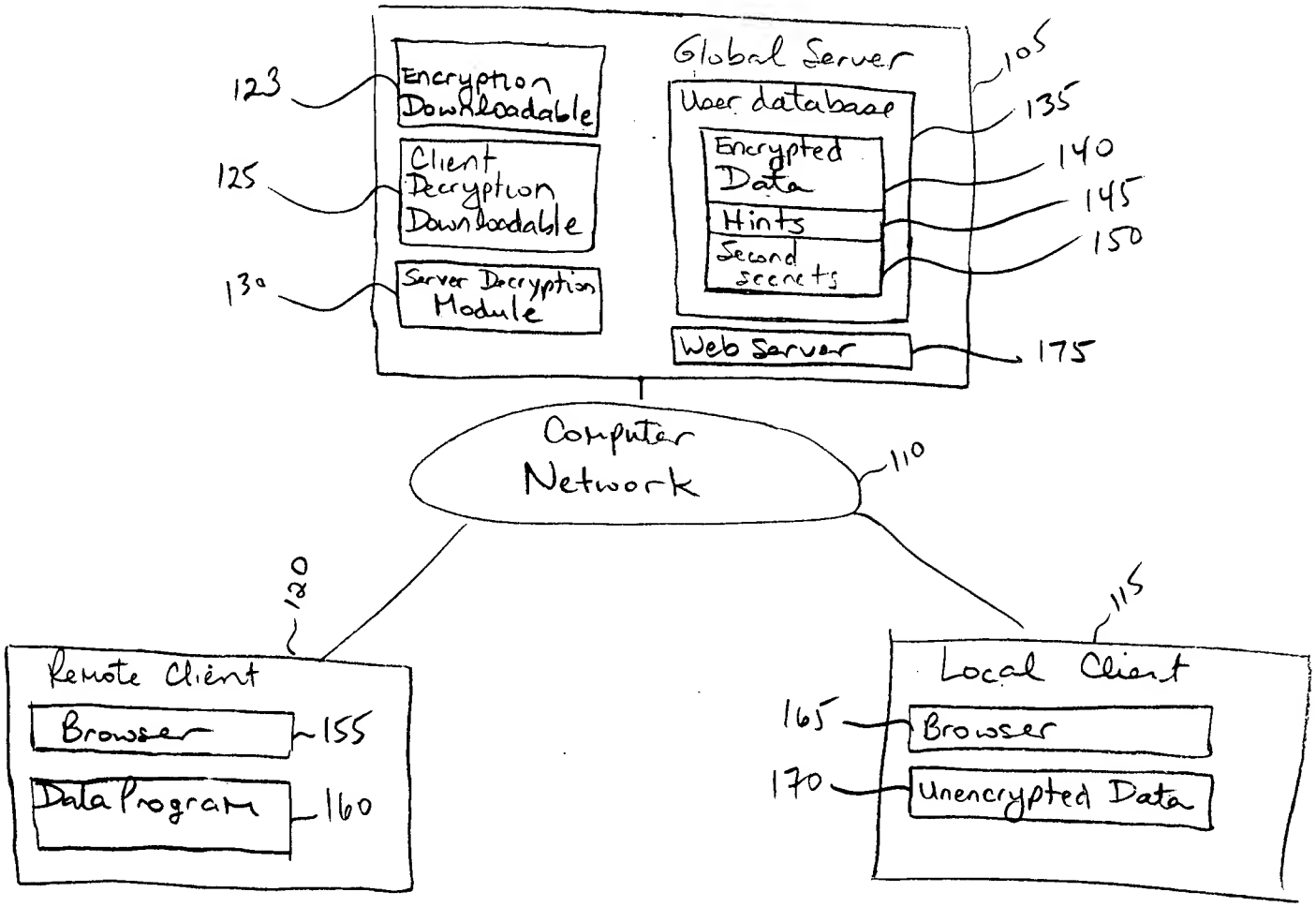

FIG. 1

09378226 . 081999

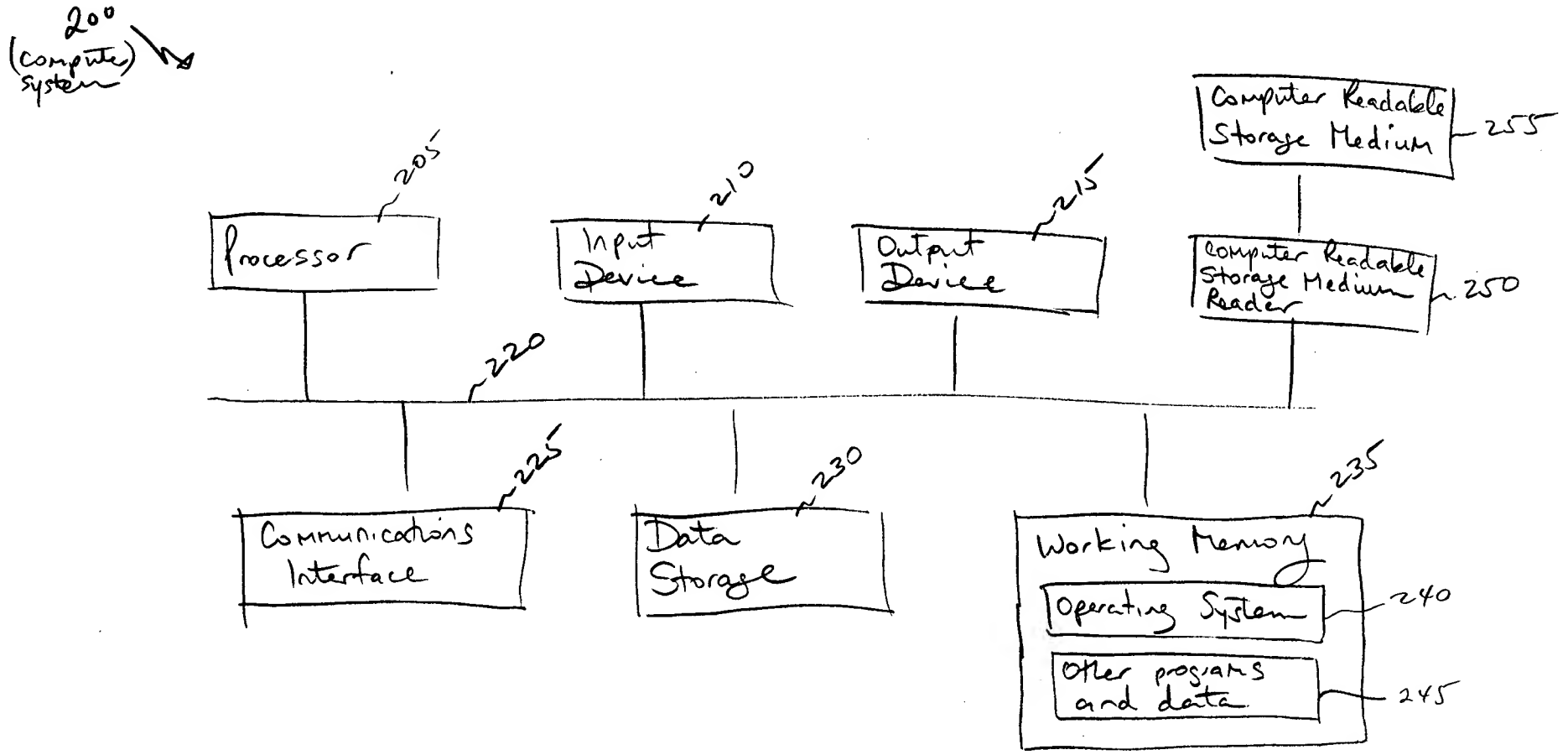

FIG. 2

09378226 . 081999

123

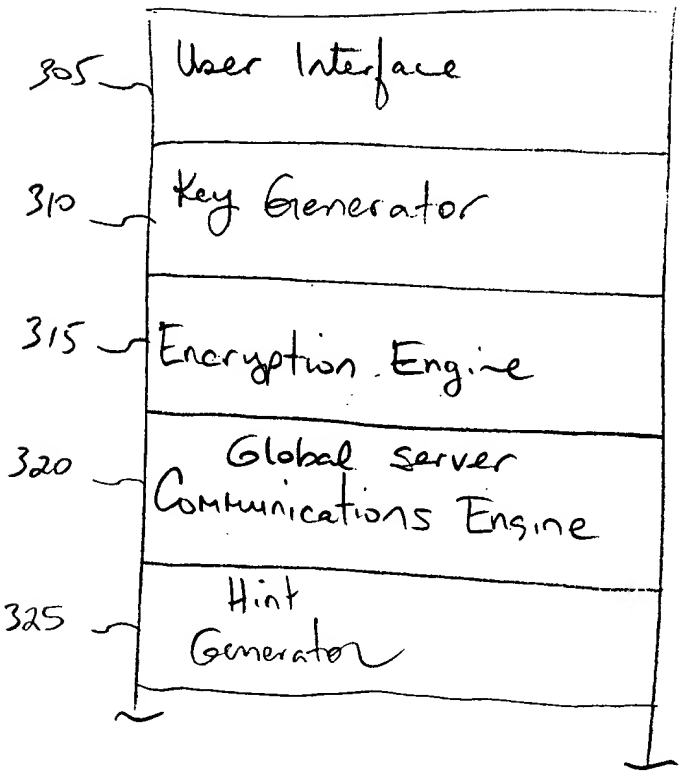

FIG. 3

(Client Encryption Downloadable)

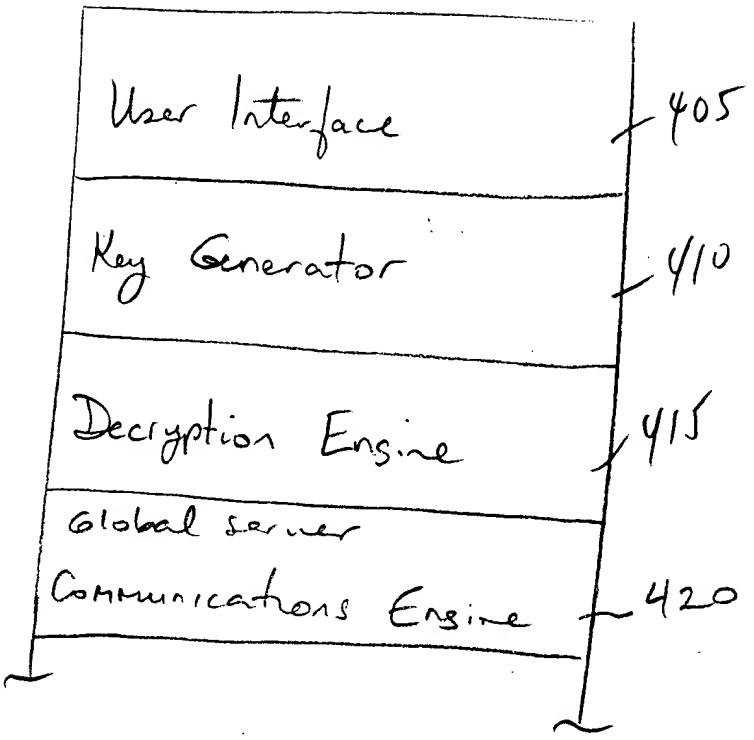

FIG 4
(Client Decryption Downloadable)

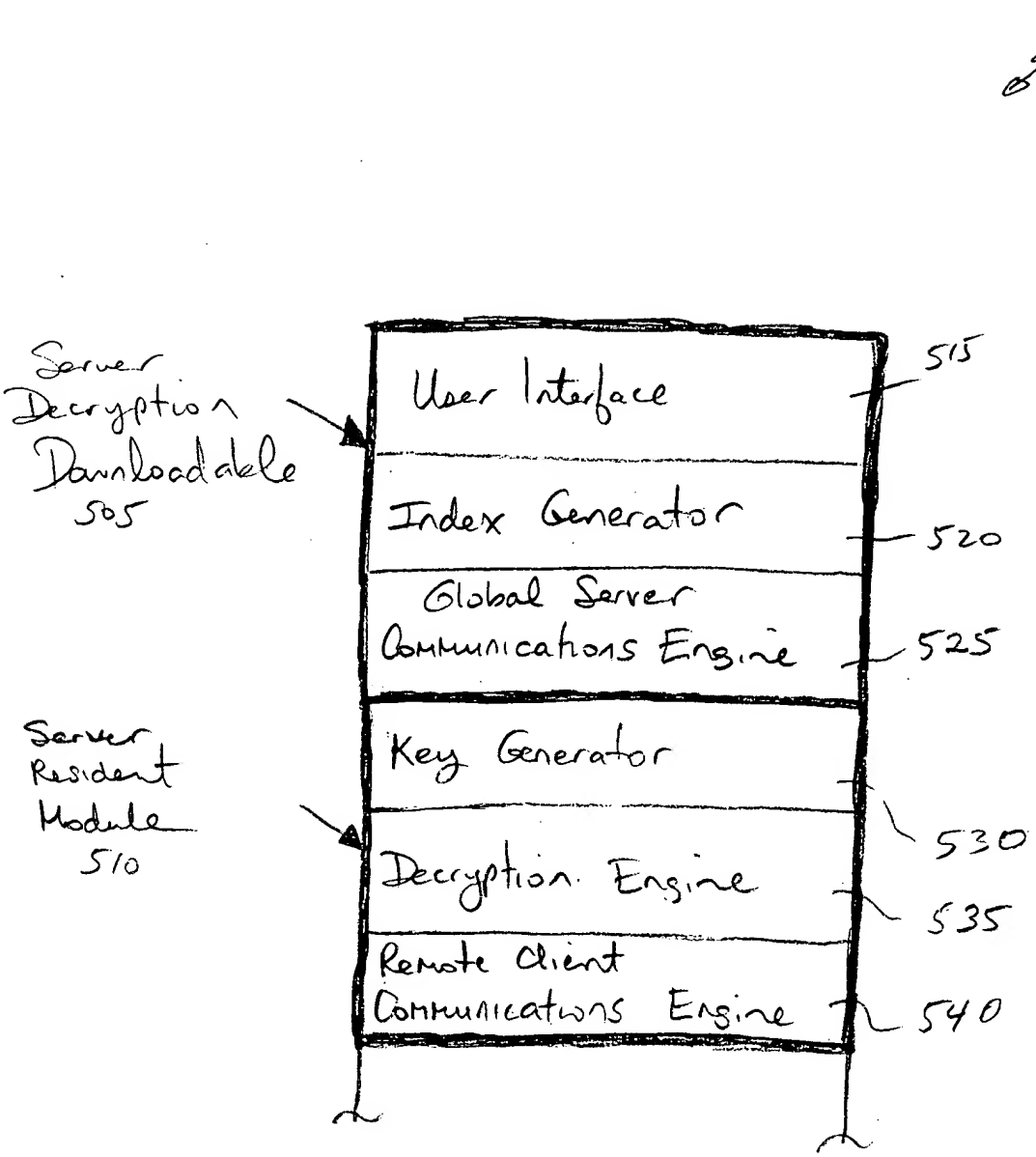

FIG. 5

(Server Decryption Module)

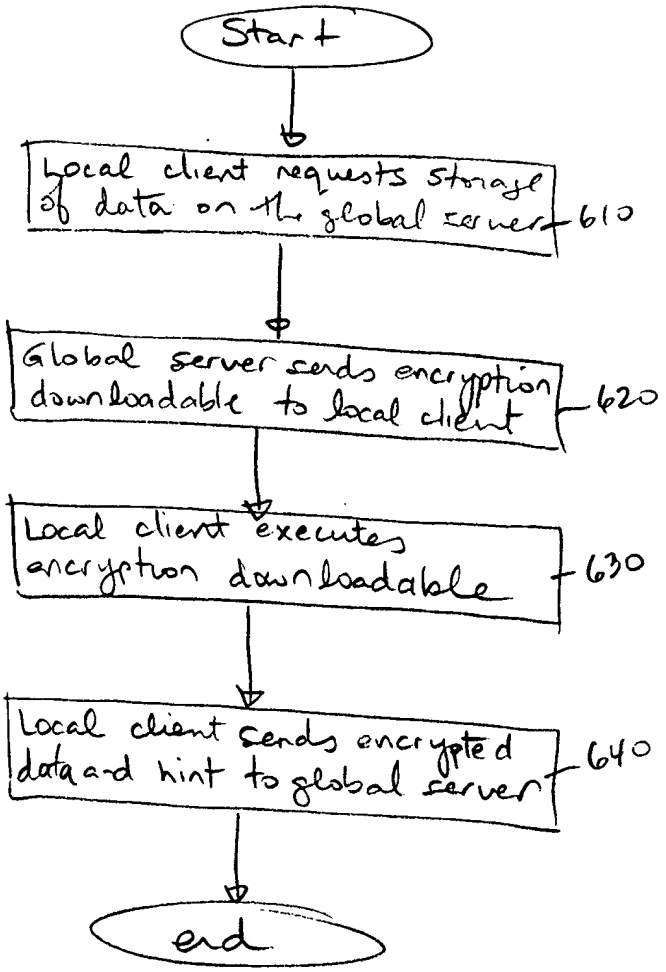

FIG. 6 (Encryption)

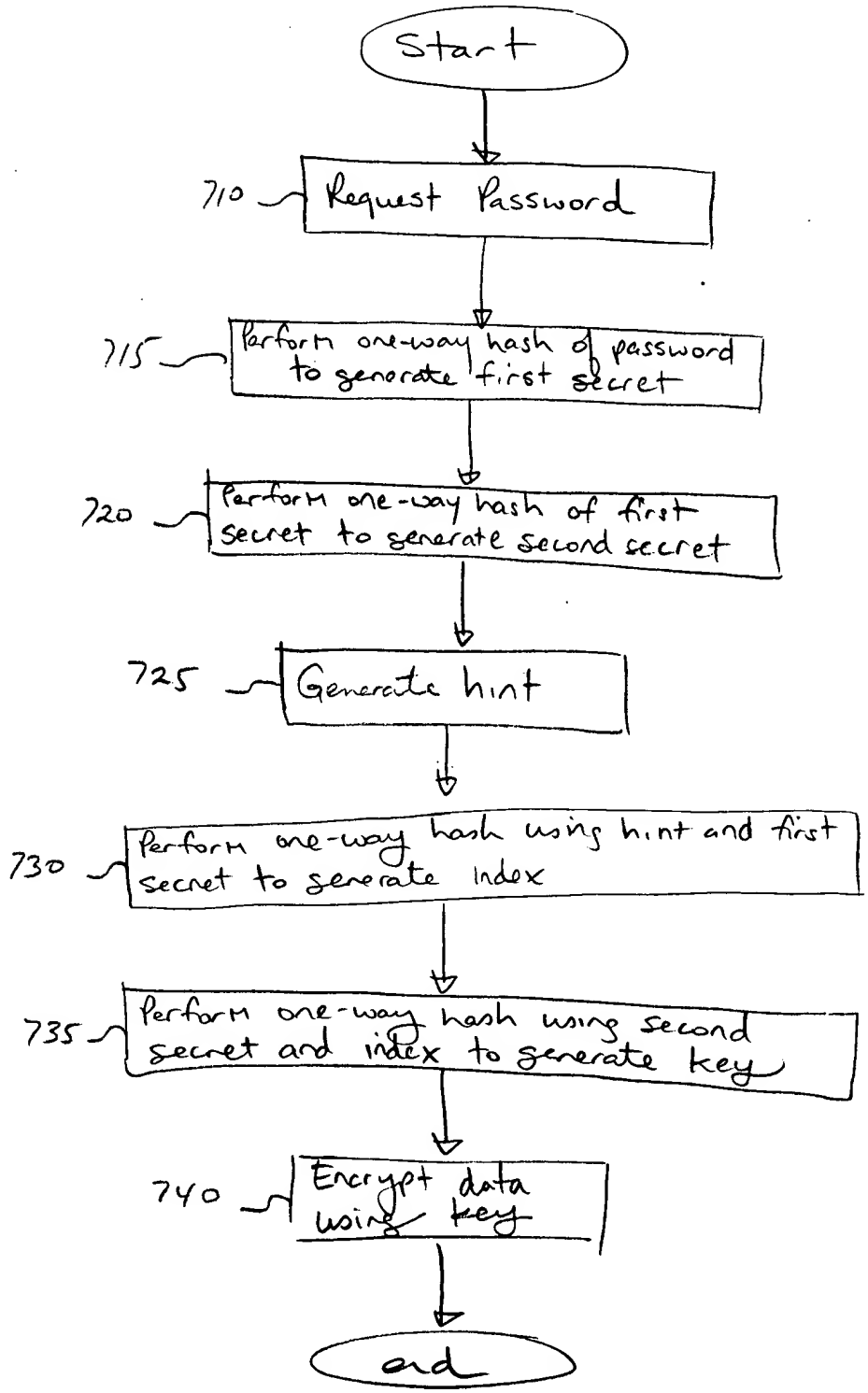
630
(Encryption Downloadable)
Start
710
Request Password
715
Perform one-way hash of password to generate first secret
720
Perform one-way hash of first secret to generate second secret
725
Generate hint
730
Perform one-way hash using hint and first secret to generate index
735
Perform one-way hash using second secret and index to generate key
740
Encrypt data using key
end

FIG. 7

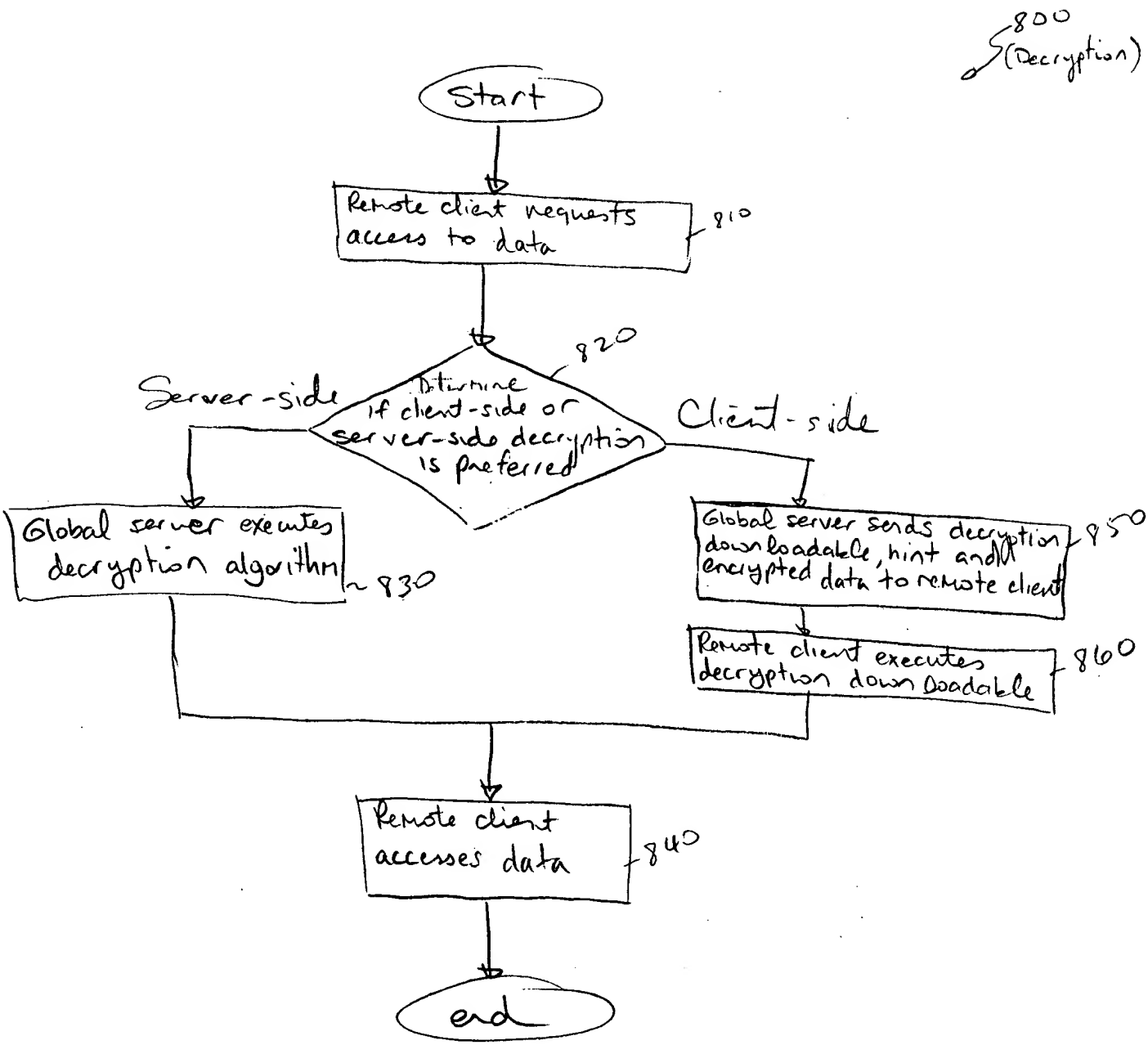
800
(Decryption)
Start
Remote client requests access to data
810
820
Determine if client-side or server-side decryption is preferred
Server-side
Client-side
Global server executes decryption algorithm
830
Global server sends decryption downloadable, hint and encrypted data to remote client
850
Remote client executes decryption downloadable
860
Remote client accesses data
840
end

FIG. 8

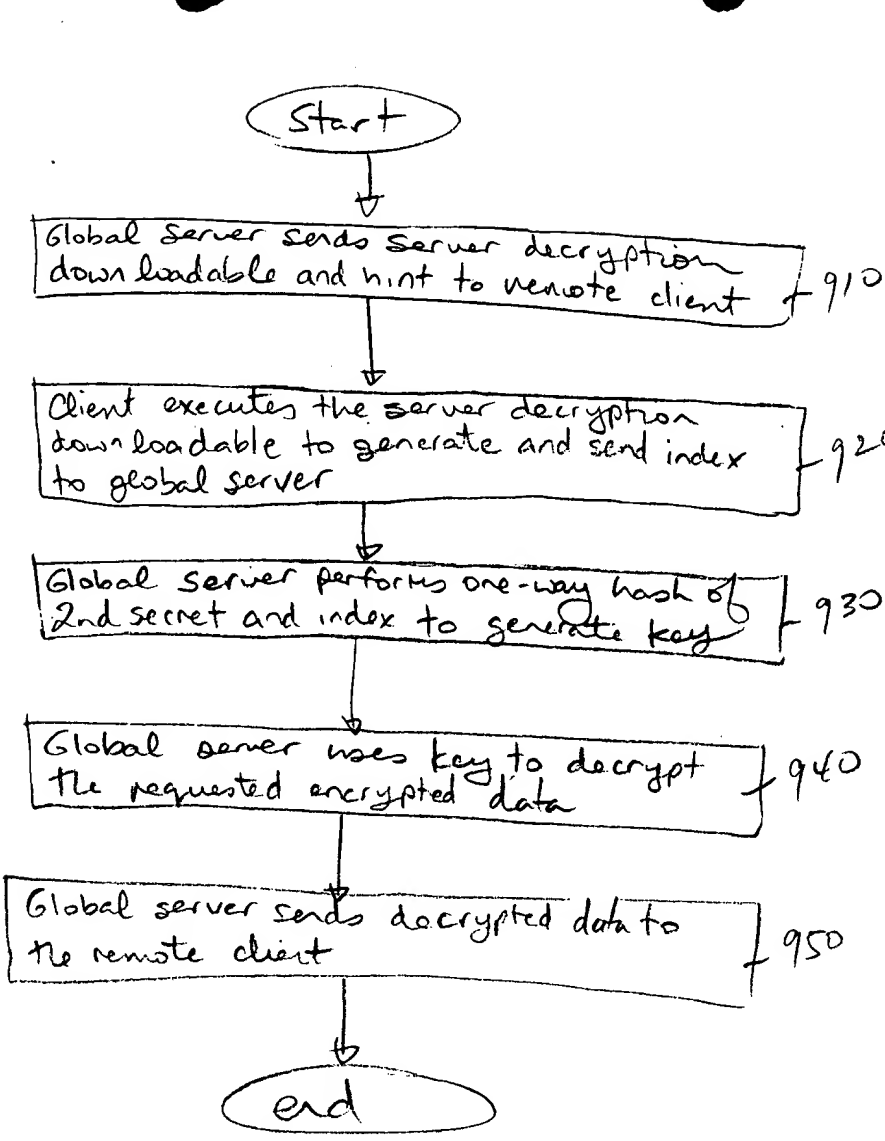
830
(Server Decryption)
Start
Global server sends server decryption downloadable and hint to remote client
910
Client executes the server decryption downloadable to generate and send index to global server
920
Global server performs one-way hash of 2nd secret and index to generate key
930
Global server uses key to decrypt the requested encrypted data
940
Global server sends decrypted data to the remote client
950
end

FIG. 9

920 (Server Decryption Downloadable)

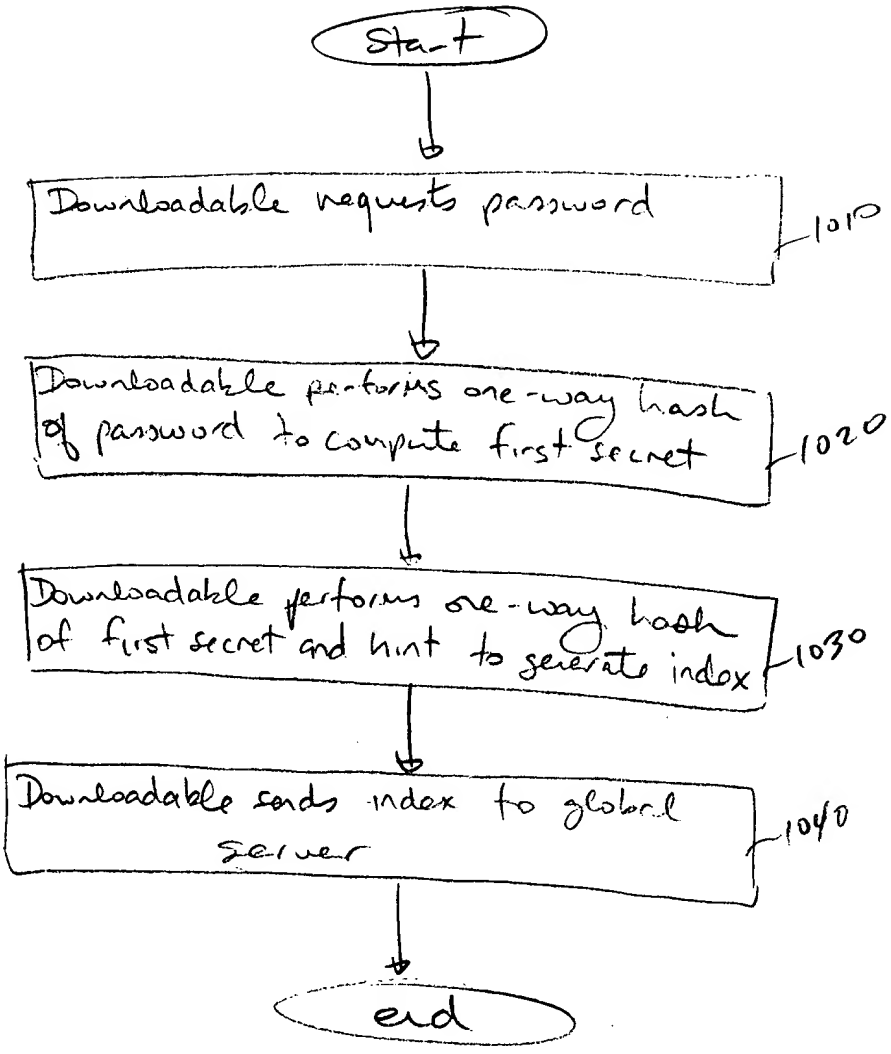

FIG. 10

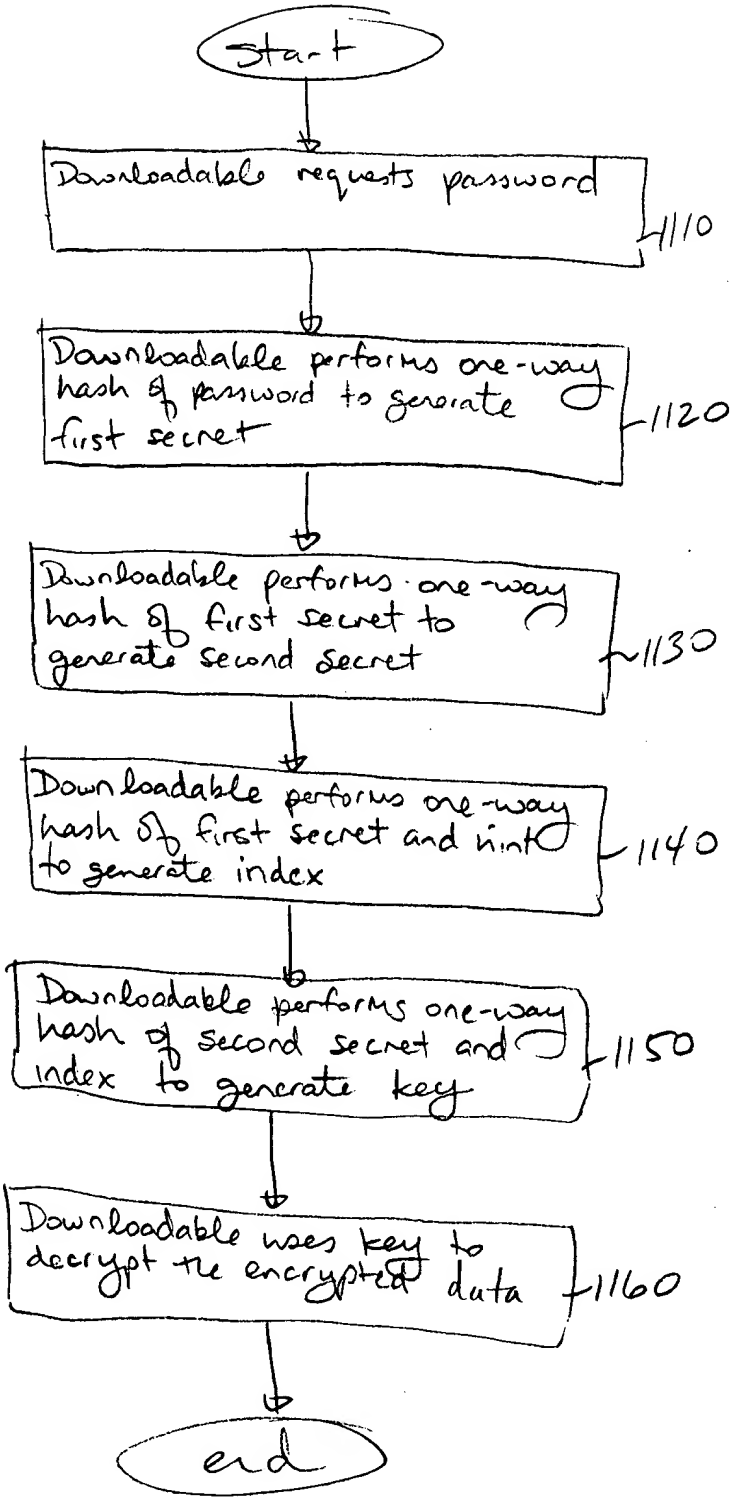
Start
Downloadable requests password
1110
Downloadable performs one-way hash of password to generate first secret
1120
Downloadable performs one-way hash of first secret to generate second secret
1130
Downloadable performs one-way hash of first secret and hint to generate index
1140
Downloadable performs one-way hash of second secret and index to generate key
1150
Downloadable uses key to decrypt the encrypted data
1160
end
860
(Remote client Decryption Downloadable)

FIG. 11

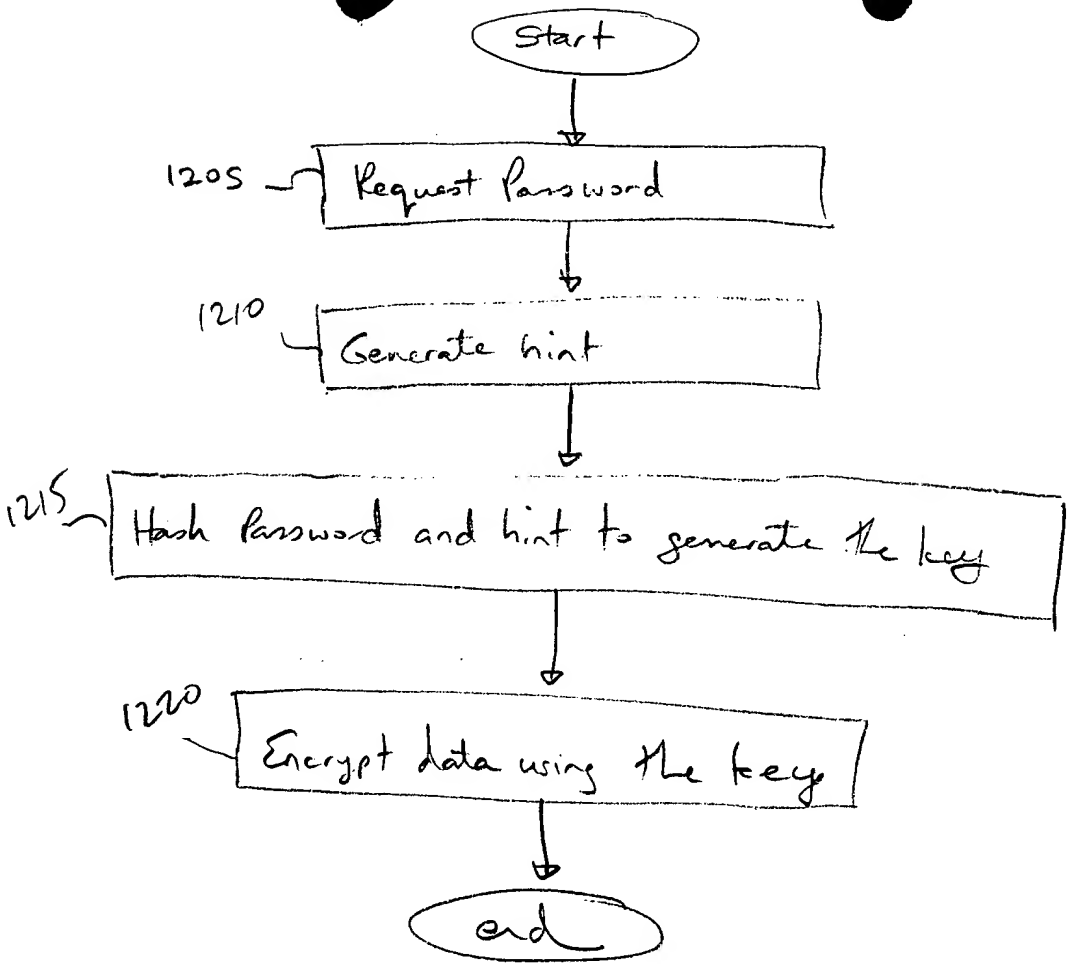
Start
1200
Encryption
1205
Request Password
1210
Generate hint
1215
Hash Password and hint to generate the key
1220
Encrypt data using the key
end

FIG. 12

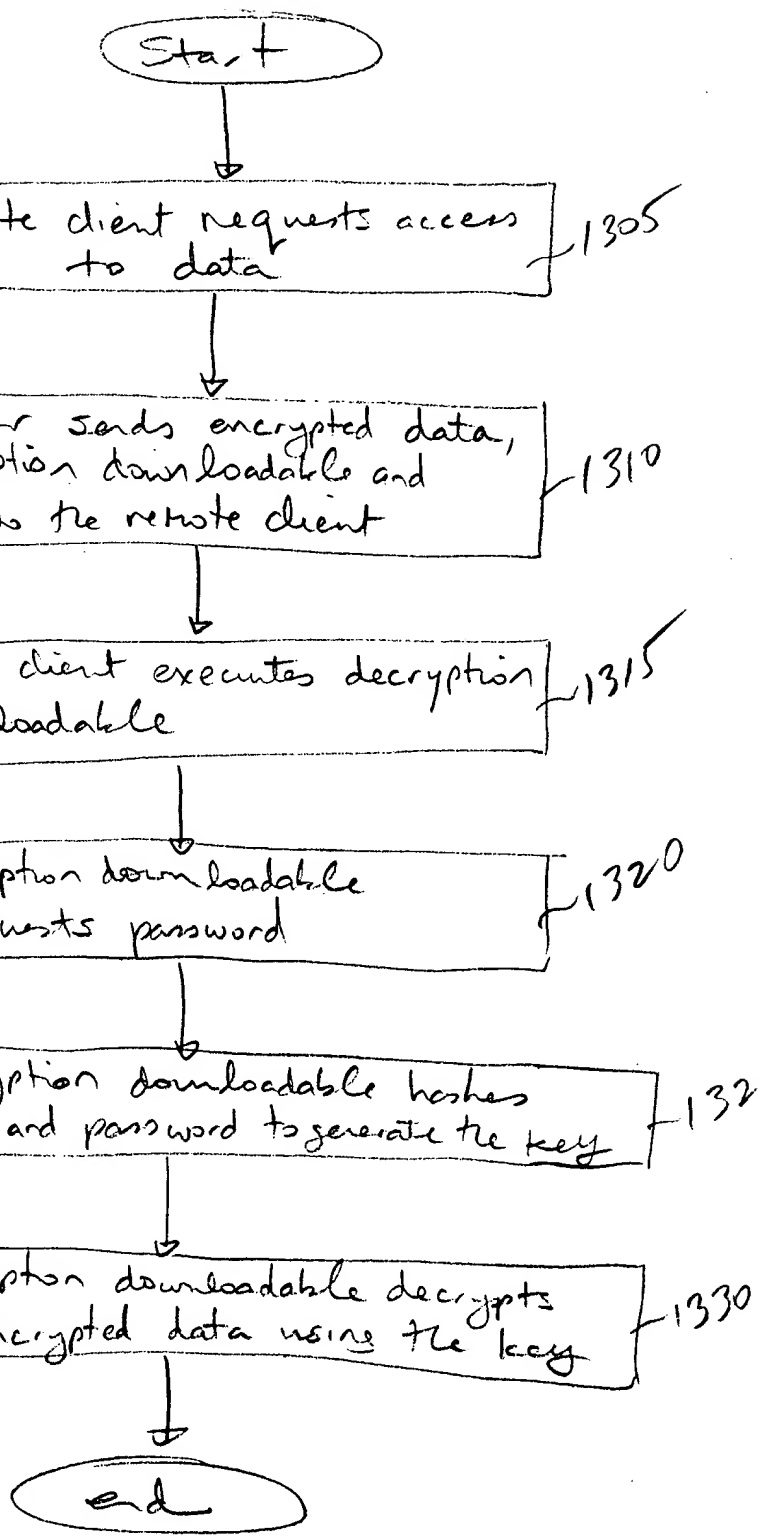
1300
Start
Remote client requests access to data
1305
Server sends encrypted data, decryption downloadable and hint to the remote client
1310
Remote client executes decryption downloadable
1315
Decryption downloadable requests password
1320
Decryption downloadable hashes hint and password to generate the key
1325
Decryption downloadable decrypts the encrypted data using the key
1330
end

FIG. 13